Remarks

At present, this disclosure is objected to because of an informality in Figure 17. Additionally, claims 1-3 stand rejected under the first paragraph of 35 U.S.C. § 112. Claim 1 stands rejected under 35 U.S.C. § 102(b) based upon the patent to Arazi (US Patent Number 5,448,639 issued on September 5, 1995). Claim 2 stands rejected under 35 U.S.C. § 102 based upon the document of Koc et al., a published United States patent application having a publication date of May 16, 2002. Lastly, claim 3 stands rejected under 35 U.S.C. § 103 based upon the aforementioned published patent application to Koc et al. In light of the amendments made herein to applicants' claims and the comments presented below, all of these rejections are respectfully traversed. Accordingly, claims 1-3 remain pending in the present application.

Initially as a matter of formality it is noted that the Examiner is correct in pointing out that the label in block 501 in Figure 17 should be labeled "N_0" as opposed to "NO". Accordingly, applicants' indicate that it is their intention to submit a corrected drawing correcting this minor informality. The drawing will be supplied as soon as practical.

Next is considered the rejection of applicants' claims 1-3 under 35 U.S.C. § 112. In his rejection the Examiner has characterized applicants' claims as failing to meet the enablement requirement. In this regard, the Examiner's attention is specifically directed to the method set forth on page 41 in applicants' specification, lines 1-9. Likewise, applicants' have set forth a method corresponding to applicants' claim 1 which is found on page 42, lines 21-29 of applicants' specification. There is nothing non-enabling about applicants' specification. The only problem is that applicants' attorney inadvertently switched the nomenclature for the first and second registers in claims 1 and 2. Again, quite inadvertently, the lower value for the variable i was indicated as being a 0 when in fact the specification clearly indicates that the value is 1. Applicants have amended claims 1 and 2 to correct all such informalities. Accordingly, with respect to claims 1 and 2 it is respectfully requested that the rejection under 35 U.S.C. § 112 be withdrawn.

Next is considered the rejection of applicants' claim 3 under 35 U.S.C. § 112. In this regard, it is to be particularly noted that applicants' have added the language which describes the first input to the adder as being the leftmost k-1 bit of the second register. This is in compliance with applicants' description as seen in their Figure 17. Additionally, it is noted that applicants' have also incorporated multiplexor 505 shown in Figure 17 in claim 3. Accordingly, any and all informalities that may have been present in claim 3 should now be eliminated. It is therefore respectfully requested that the rejection of applicants' claim 3 under the first paragraph of 35 U.S.C. § 112 also be withdrawn.

Attention is now turned to the art based rejections of applicants' claims 1-3. All of these rejections are respectfully but strenuously traversed. It is further noted that with respect to the rejection under 35 U.S.C. § 102 these are narrow grounds of rejection. Rejections under 35 U.S.C. § 102 require each and every claim element to be found within the four corners of a single cited document. Furthermore, these claim elements must be combined in the same way and perform the same function as is recited in applicants' claims. Neither of the rejections under 35 U.S.C. § 102 satisfy this requirement.

With respect to the rejection of applicants' claim 1 under 35 U.S.C. § 102 based upon the patent to Arazi, the Examiner's attention is directed to column 10, lines 17-45. This is the portion of the cited patent that deals with calculations relating to modular inverses. It is noted that the method taught by Arazi specifically requires a table lookup (line 21). No such step is recited in applicants' claim 1. Furthermore, applicants' claim 1 specifically recites a shifting step. No shifting step is shown in this portion of the patent to Arazi. Likewise, Arazi does not teach the steps for calculating "$S = S + 2^i$ and $Q = Q + A$". These are two computations effectively carried out in step (c) of applicants' claim 1. Not only are these steps not carried out in the patent to Arazi, Arazi does not appear to make any attempt to determine what is in a rightmost bit position of any of his variables in the steps that he shows for his method 5 for calculating modular inverses. It is therefore seen that not only does Arazi fail to include a

number of essential elements recited in applicants' claim 1, it is seen that Arazi ultimately teaches away from the simplified approach provided by the present applicants. Accordingly, it is seen that the rejection of applicants' claim 1 under 35 U.S.C. § 102(b) based upon the patent to Arazi cannot be sustained. It is therefore respectfully requested that it be withdrawn.

Attention is next directed to the rejection of applicants' claim 2 under 35 U.S.C. § 102(e) based upon the published US patent application to Koc et al. In this regard, the Examiner points to paragraph 63 from the subject publication. From the start, it is noted that what is indicated there is not what applicants' are claiming. In particular, it is noted that Koc et al. refer to the calculation of the "negative of the multiplicative inverse of the LSW of p modulo 2^w". As used by Koc et al., LSW stands for Least Significant Word (paragraph 19 of the subject publication). In this respect, it is noted that applicants' claimed process generates the negative of the multiplicative inverse not merely the least significant word of the inverse. Even apart from this, it is seen that in the method set out in paragraph 64 and as elaborated upon in Table 5 from Koc et al., the process described is significantly different than that which is recited in applicants' claim 2. Applicants' claim 2 is a recursive application of a 3 step method. Nothing even slightly so simple can be seen in Table 5 from Koc et al. In particular, Koc et al. describe multiple loops that are carried out in a serial fashion. In contrast, applicants' only have a single loop. Furthermore, applicants' claimed process involves only steps of addition and subtraction. In contrast, the Examiner's attention is directed to step 6 shown in Table 5 of the patent to Koc et al. where 3 additions and a multiplication are required. No multiplication is required in applicants' claimed process. Furthermore, there is no teaching, disclosure or suggestion in the patent to Koc et al. that anything as simple as applicants' recited process would be effective. In utter contrast it is seen that the process recited in Koc et al. is long, involved and extremely cumbersome. Those of ordinary skill in the art following the teachings of Koc et al. would not in any way be lead to employ the process recited by the present applicants. In particular, it is seen that those of ordinary skill in the art would be required to employ steps which require multiplicative operations. It is therefore seen that the rejection of applicants' claim 2 under 35

U.S.C. § 102(e) based upon the published patent application to Koc et al. cannot be sustained. Likewise, it is respectfully but strenuously requested that this rejection be withdrawn.

Lastly, the rejection of applicants' claim 3 under 35 U.S.C. § 103 is considered. In this regard, it is noted that applicants' claim 3 is generally directed to a circuit for determining the negative multiplicative inverse of an odd binary number *A*. To the extent that any such similar method is shown in the patent to Koc et al. in their paragraphs 63 and 64, it is noted that any cited processes for this determination are significantly different. In particular, it is noted that the claimed circuit in applicants' specification operates in a particular fashion based upon the counter which ranges from 1 to k-1. In applicants' invention there is but a single passage between these values. In utter contrast, it is seen that Table 5 of the patent to Koc et al. incorporates at least 5 different iterative loops operating in a serial fashion. This is clearly not the same process, nor would the process described by Koc et al. having these five separate and iterative loops, lead one to employ a circuit having only one such loop. Again, it is seen that those of ordinary skill in the art having the patent to Koc et al. before them would not in any way be lead to the circuit recited in applicants' claim 3. While some of applicants' claimed elements are standardly employed in digital signal processing, there is utterly no teaching, disclosure or suggestion that such circuits are connected or connectable in the same way as recited in applicants' claim 3, based upon the teachings found in Koc et al. Again, it is respectfully requested that the rejection of applicants' claim 3 under 35 U.S.C. § 103 also be withdrawn.

It is noted that the amendments being made herein are being made as of right. It is also noted that the amendments made herein per se do not require the payment of any additional fees. However, it is noted that applicants' are requesting a one month extension of time with respect to the submission of this response. Unfortunately, this delay was necessitated by other pressing matters, including the inventors schedules.

No amendment made was related to the statutory requirements of patentability unless expressly stated herein. No amendment made was for the purpose of narrowing the scope of any claim, unless applicants have argued herein that such amendment was made to distinguish over a particular cited document or combination of documents.

Accordingly, it is now seen that all of the applicants' claims are in condition for allowance. Therefore, early notification of the allowability of applicants' claims is earnestly solicited. Furthermore, if there are any other matters which the Examiner feels could be expeditiously considered and which would forward the prosecution of the instant application, applicants' attorney wishes to indicate his willingness to engage in any telephonic communication in furtherance of this objective. Accordingly, applicants' attorney may be reached for this purpose at the numbers provided below.

Respectfully Submitted,

Dec. 16, 2004
Date

Lawrence D. Cutter
LAWRENCE D. CUTTER, Senior Attorney
Reg. No. 28,501

IBM Corporation, IP Law Dept.
2455 South Rd., M/S P386
Poughkeepsie, NY 12601

Phone: (845) 433-1172
FAX: (845) 432-9786
EMAIL: cutter@us.ibm.com